US-VISIT Program, Increment 1
Privacy Impact Assessment
Executive Summary

December 18, 2003

Contact Point

Steve Yonkers
US-VISIT Privacy Officer
Department of Homeland Security
(202) 298-5200

Reviewing Official

Nuala O'Conner Kelly
Chief Privacy Officer
Department of Homeland Security
(202) 772-9848

US-VISIT Program, Increment 1
Privacy Impact Assessment
Executive Summary

Overview

US-VISIT, the United States Visitor and Immigrant Status Indicator Technology, is a legislatively-mandated DHS program that is designed to:

- Enhance the security of American citizens, permanent residents, and visitors
- Expedite legitimate travel and trade
- Ensure the integrity of the immigration system
- Safeguard the personal privacy of visitors

When fully implemented, US-VISIT will provide a dynamic, interoperable system involving numerous stakeholders across the government. Increment 1, as the name suggests, is the first step in the implementation process. Increment 1 proposes to integrate and modify the capabilities of several information systems in order to accomplish the mission of US-VISIT.

This Privacy Impact Assessment (PIA) focuses on Increment 1 of this entry exit system.

What Information is Collected

The US-VISIT program will collect and retain biographic, travel, and biometric information (i.e., photograph and fingerprints) pertaining to visitors.

Individuals covered by Increment 1 ("covered individuals") are nonimmigrant visa holders traveling through air and sea ports.[1] The DHS regulations and related Federal Register notice for US-VISIT Increment 1 will fully detail coverage of the program.

Why the Information is Being Collected and Intended Use of the Information

In accordance with Congressional mandates for an entry exit system, information is collected from and used to verify the identity of covered individuals who enter or leave the United States. This enables U.S. authorities to enhance the security of the United States by more effectively identifying covered individuals who are:

- Known to pose a threat or are suspected of posing a threat to the security of the United States;
- Known to have violated the terms of their admission to the United States; or
- Wanted for commission of a criminal act in the United States or elsewhere.

[1] Nonimmigrant visa entrants comprise a small percentage of the 330 million non-citizens admitted annually through ports of entry. Establishing US-VISIT incrementally with this population will allow DHS to test implementation of the system and to make revisions as needed for future increments.

Information Access and Sharing

Information collected and retained by US-VISIT will be accessed by employees of DHS components—Customs and Border Protection, Immigration and Customs Enforcement, Citizenship and Immigration Services, and the Transportation Security Administration—and by consular officers of the Department of State. Strict security controls will be put in place to ensure that only those personnel with a need for the information in the performance of their official duties will be able to access information in the system.

If necessary, the information that is collected will be shared with other law enforcement agencies at the federal, state, local, foreign, or tribal level, who are lawfully engaged in collecting law enforcement intelligence information and who need access to the information in order to carry out their law enforcement duties.

Consent Mechanisms

The admission into the United States of an individual subject to US-VISIT requirements will be contingent upon submission of the information required by US-VISIT, including biometric identifiers. A covered individual who declines to provide biometrics is inadmissible to the United States, unless a discretionary waiver is granted under section 212(d)(3) of the Immigration and Nationality Act. Such an individual may withdraw his or her application for admission, or be subject to removal proceedings.

Security

Information accessible to US-VISIT will be protected through multi-layer security mechanisms that are physical, technical, administrative and environmental and that are in compliance with the DHS IT Security Program Handbook and DHS Baseline Security Requirements for Automated Information Systems. These security mechanisms provide access control to sensitive data, physical access control to DHS facilities, confidentiality of communications, authentication of sending parties, and careful screening to ensure that all personnel with access to data are screened through background investigations commensurate with the level of access required to perform their duties.

System of Records

A system of records notice (SORN)—normally required under the Privacy Act—is not necessary for US-VISIT because no new system is being developed for Increment 1. However, the ADIS and IDENT SORNs have been revised to reflect US-VISIT usage.

Although US-VISIT derives its capability from the integration and modification of existing systems, it nevertheless represents a new business process that involves new uses of existing data and the collection of new data items. As a result, there is a potential for new privacy risks, which are addressed in the PIA.

Privacy Controls

US-VISIT collects, integrates, and shares personal information of covered individuals. Covered individuals must consent to the collection, use, and disclosure of this personal information if they wish to enter or leave the U.S.

To address the privacy concerns associated with the program, US-VISIT will implement comprehensive privacy controls, which will be modified and updated as the system is revised and expanded. These controls consist of:

- Public education through transparency of the program, including development and publication of a Privacy Policy that will be disseminated prior to the time information is collected from potential visitors;[2]
- Establishment of privacy sensitivity awareness programs for US-VISIT operators[3];
- Establishment of a Privacy Officer for US-VISIT and implementation of an accountability program for those responsible for compliance with the US-VISIT Privacy Policy;
- Periodic strategic reviews of US-VISIT data to ascertain that the collection is limited to that which is necessary for US-VISIT stated purposes;
- Usage agreements between US-VISIT and other agencies authorized to have access to US-VISIT data;
- To the extent permitted by law, regulations, or policy, establishment of opportunity for covered individuals to have access to their information and/or allow them to challenge its completeness;
- Maintenance of security safeguards (physical, electronic and procedural) consistent with federal law and policy to limit access to personal information only to those with appropriate rights, and to protect information from unauthorized disclosure, modification, misuse, and disposal, whether intentional or unintentional; and
- Establishment of administrative controls to prevent improper actions due to data inconsistencies from multiple information sources.

Contact Point and Reviewing Official

Contact Point:	Steve Yonkers US-VISIT Privacy Officer (202) 298-5200
Reviewing Official:	Nuala O'Conner Kelly Chief Privacy Officer, DHS (202) 772-9848

Comments

We welcome your comments on this privacy impact assessment. Please write to: Privacy Office, Attn.: US-VISIT PIA, U.S. Department Of Homeland Security, Washington, DC 20528, or email privacy@dhs.gov. Please include US-VISIT PIA in the subject line of the email.

[2] A copy of the Privacy Policy is appended to this report.

[3] The legacy systems on which Increment 1 is built include privacy sensitivity training requirements. This training will be made mandatory for US-VISIT operators.